TRUSTWAVE SIEM FOR GOVERNMENT

EASY COMPLIANCE, ENHANCED SECURITY

Trustwave Security Information and Event Management (SIEM) is a log and threat management solution providing government agencies with the ability to automate their existing continuous network monitoring capabilities, correlate and analyze critical security-related information, and enhance risk-based decision making at the agency and enterprise level.

Security Information and Event Management (SIEM) investments are often driven by the need to quickly address regulatory compliance issues. As agencies overcome the compliance hurdle, they increasingly use SIEM to improve security monitoring capabilities to manage escalating threats. Most agencies desire baseline SIEM Solutions that offer near real-time collection and analysis of log data from host systems, security devices and network devices. Also, agencies want a solution that supports long-term storage and reporting and that supports their needs without extensive customization.

Whether selecting a SIEM solution for regulatory compliance reporting (i.e. FISMA), threat management, or both, Trustwave offers a portfolio of solutions to give every government agency the ability to address the enterprise-wide risk management process, providing the capability to assess, monitor, and respond to risk on an ongoing basis. Trustwave offers government agencies a Continuous Monitoring and Risk Mitigation capability by providing the means to detect, respond to, and mitigate cyber incidents.

Threats to cyber security systems are evolving and growing. Targeted attacks and Advanced Persistent Threats (APT's) are on the rise and pose increasing risks to critical infrastructure and government information systems. Adversaries possess sophisticated levels of expertise and significant resources to attain their objective of breaching networks over extended periods of time. Continuous monitoring and adjustment of security controls to keep up with these threats are essential to protect government networks. Security personnel need the near real-time security status of their systems, and their executive leadership needs up-to-date assessments in order to make risk-based decisions.

EFFECTIVE COMPLIANCE AND SECURITY

Indicators of compliance and policy violations, network health issues and security threats are hidden in terabytes of log data. Whatever the compliance initiatives may be, SIEM satisfies the log management mandate of regulatory standards or internal security policies. These include:

- Federal Information Security Management Act (FISMA)
- Payment Card Industry Data Security Standard (PCI DSS)
- DoD Information Assurance Certification and Accreditation Process (DIACAP)
- NIST SP 800-53
- NIST 800-37 CM
- Executive Order on Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21
- Health Insurance Portability and Accountability Act (HIPAA)

EFFICIENT LOG COLLECTION AND PROCESSING

Trustwave SIEM solutions collect and process all log data from audit sources at consistently high speeds. Trustwave SIEM is scalable to handle large volumes of data to include unpredictable increases. Raw and parsed data is available for customers to view and for the SIEM to analyze. Trustwave includes forensic grade hash comparisons for non-repudiation of data and also stores raw message logs in their entirety (versus truncated), making them defendable and admissible as evidence for cases requiring litigation. Trustwave parsing technology allows for high-quality reports and enables visual analysis of events, and makes correlation and dashboard summarization of big data possible for advanced and actionable analytics.

Adhering to forensic quality standards, Trustwave Security Data Warehouse™ will file, secure, monitor and retain all log data to satisfy regulatory standards using highly optimized data compression, indexing techniques, and flexible retention and expiry options to meet varying requirements.

LOGGING JUST GOT SMARTER

Many choices exist for collecting, storing and processing logs. More useful than simply collecting logs, however, is finding the important information hidden within these volumes from across your organization. Continuous, efficient and high-speed parsing and correlation uncover the hidden information and risks. Trustwave Log Management Enterprise appliances offer a head start on eliminating false positives, isolating threats, enabling investigations, and doing something about them.

A SIEM DEVICE FOR ALL

Trustwave Log Management Appliances are ideal for government networks needing a self-managed log and event management solution.

A ONE-STOP DASHBOARD

From the configurable SIEM dashboard, simply point and click to begin an investigation, or run a comprehensive report on any monitored device. The advantage of normalized events over native logs is the speed of doing inquiries, as well as investigations and running reports. Log detail remains available while normalized events bubble up useful contextual information faster for continuous monitoring of government networks.

Anywhere log management:

Implementations range from one appliance to a hierarchical deployment of multiple appliances to enterprise-grade SIEM software which aligns with remote geographic sites or to meet separation of data requirements. Trustwave SIEM solutions accept logs directly from hundreds of vendors and sources or from other SIEM solutions.

Trustwave SIEM solutions offer strong ROI. We include compliance reporting, our self-maintaining Security Data Warehouse™ (SDW) and device support for audit sources. Also, agencies can add new devices without incremental licensing fees. Centralized logging and event management has never been easier with Trustwave SIEM solutions.

Sensibly sized:

Choose one of the six configurations available for Trustwave Log Management Appliances and get the needed capacity and functionality in one appliance. Trustwave appliances are built on a hardened and optimized Linux OS, locked down for secure access, and Common Criteria certified at EAL 3+. Software updates and configuration changes are made through a Web-based graphical user interface.

Easy research:

Use the Event Explorer to conduct pre-incident research by searching parsed events stored in compressed form in the Security Data Warehouse™ (SDW). Event Explorer can also be used for troubleshooting, tracking user activity and forensic investigation.

Trustwave®

Smart security on demand

For more information: https://www.trustwave.com.

COMMITTED TO YOUR SUCCESS

Trustwave solutions have a low total cost of ownership. Primarily agent-less data collection reduces the burden on infrastructure. The unique Security Data Warehouse™ (SDW) embeds a self-managing relational database requiring no database administrator. The warehouse compresses raw and parsed logs, minimizing the impact on storage budgets. The product architecture is scalable as more data sources are added or as risk policies evolve. Trustwave includes compliance and security reports, metrics and correlations, delivering visibility and security expertise for analysis, reporting and compliance.

FLEXIBLE DEPLOYMENT OPTIONS

Trustwave SIEM solutions flexible deployment options lead the industry, enabling government customers to meet both business and technical requirements. Options include a traditional approach of perpetual licensing and a subscription-based option available as a Trustwave Managed Security Services offering that serves budget-conscious customers desiring a Software-as-a-Service model. The Cloud-based security and compliance management platform delivers the same benefits to agencies with concerns over combating advanced persistent threats (APTs) without the need of a fully-staffed security operations center.

KEY BENEFITS OF TRUSTWAVE SIEM SOLUTIONS

- A complete set of FISMA reports. The reporting service automates scheduling and report distribution, and includes a repository to archive reports addressing FISMA requirements.
- Verification that controls are enforcing audit and compliance policy through alerting, notifications, reports, dashboards, and core investigative capabilities of the solution.
- Alerts reduce false positives. The automated portions of the system provide the ability to prioritize alerts based on impact to compliance and/or organization operations.
- Dashboards and reports are key performance indicators used to measure security value and are especially useful in justifying budgets.
- Easily adapts to changing requirements; and scales as event volumes change.